

Dixon's Theorem and random synchronization

Peter J. Cameron
 School of Mathematical Sciences
 Queen Mary, University of London
 Mile End Road
 London E1 4NS, U.K.

Abstract

A transformation monoid on a set Ω is called *synchronizing* if it contains an element of rank 1 (that is, mapping the whole of Ω to a single point). In this paper, I tackle the question: given n and k , what is the probability that the submonoid of the full transformation monoid T_n generated by k random transformations is synchronizing?

The question has some similarities with a similar question about the probability that the subgroup of S_n generated by k random permutations is transitive. For $k = 1$, the answer is $1/n$; for $k = 2$, Dixon's Theorem asserts that it is $1 - o(1)$ as $n \rightarrow \infty$ (and good estimates are now known). For our synchronization question, for $k = 1$ the answer is also $1/n$; I conjecture that for $k = 2$ it is also $1 - o(1)$.

Following the technique of Dixon's theorem, we need to analyse the maximal non-synchronizing submonoids of T_n . I develop a very close connection between transformation monoids and graphs, from which we obtain a description of non-synchronizing monoids as endomorphism monoids of graphs satisfying some very strong conditions. However, counting such graphs, and dealing with the intersections of their endomorphism monoids, seems difficult.

Keywords: transformation monoid, synchronization, graph homomorphisms, random generation.

1 Dixon's Theorem

In 1969, John Dixon [3] proved the following theorem:

Theorem 1.1 *The probability that two random permutations in the symmetric group S_n generate S_n or A_n is $1 - o(1)$ as $n \rightarrow \infty$.*

In fact, good estimates are known. Babai [1] showed that the probability is $1 - 1/n + O(1/n^2)$: the term $1/n$ arises from the probability that the two permutations have a common fixed point. Several further terms of the asymptotic expansion are known.

It is my purpose here to begin a similar analysis for the *full transformation monoid* T_n on the set $\Omega = \{1, \dots, n\}$. Things are a little different, since T_n requires three generators. (If the monoid M is generated by a set S of transformations, then the group of permutations in M is generated by the permutations in S ; so if $M = T_n$ with $n > 2$, then S must contain at least two permutations, and at least one non-permutation.) Indeed, since permutations are exponentially scarce in T_n , we have to choose a huge number of random elements in order to generate T_n with high probability.

Further analysis of Dixon's theorem suggests a different approach. The first, and easier, step is to calculate the probability that two permutations in S_n generate a transitive subgroup. If c_n is the number of pairs of elements of S_n which generate a transitive subgroup, then counting pairs according to the orbit of the point 1 of the group they generate gives

$$\sum_{k=1}^n \binom{n-1}{k-1} c_k ((n-k)!)^2 = (n!)^2,$$

a recurrence relation from which c_n can be determined. It is then easy to show that $c_n/(n!)^2 = 1 - 1/n + O(1/n^2)$.

However, a cruder analysis is more useful in other situations. The maximal intransitive subgroups of S_n have the form $S_k \times S_{n-k}$ for $1 \leq k \leq \lfloor n/2 \rfloor$. If two elements fail to generate a transitive subgroup, then they lie in some maximal intransitive subgroup; the probability of this is at most

$$\frac{1}{(n!)^2} \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{k} (k!)^2 ((n-k)!)^2 = \frac{1}{n} + O\left(\frac{1}{n^2}\right).$$

The remainder of the proof of Dixon's Theorem involves showing that the probability that the two permutations lie in a transitive subgroup other

than the symmetric or alternating group is very small. This probability is estimated similarly to the above, by bounding the number and order of maximal transitive subgroups other than S_n and A_n .

We note in passing that the probability that a single random permutation in S_n generates a transitive subgroup is $1/n$. For the permutations which generate transitive subgroups are the n -cycles, and it is well-known that there are exactly $(n-1)!$ of these.

2 Synchronizing monoids

Let T_n be the full transformation monoid on the set $\Omega = \{1, \dots, n\}$, consisting of all *endofunctions* $f : \Omega \rightarrow \Omega$, with the operation of composition. A *transformation monoid* is a submonoid of T_n .

A transformation monoid M is said to be *synchronizing* if it contains an element of rank 1 (that is, a function whose image has cardinality 1). It seems that synchronizing monoids behave a little like transitive subgroups of S_n . The first observation gives an exact parallel:

Proposition 2.1 *The probability that a random endofunction generates a synchronizing monoid is $1/n$.*

Proof The endofunction f generates a synchronizing monoid if and only if it has a unique periodic point. Such a function is defined by a rooted tree, with edges directed towards the root. There are n^{n-1} rooted trees, and n^n endofunctions altogether.

I conjecture that the probability that two random endofunctions generate a synchronizing monoid is $1 - o(1)$. The strategy is to describe the maximal non-synchronizing monoids, and then to argue as in the proof of Dixon's theorem. The first part of the programme is realised here, and some evidence towards the second is given.

Of course, the analogy between transitive subgroups and synchronizing submonoids is not perfect. Luczak and Pyber [4] showed that the proportion of elements of S_n which lie in transitive subgroup of S_n except S_n and possibly A_n is $1 - o(1)$, though the rate of convergence is not well understood. However, every element of T_n lies in a proper synchronizing submonoid. For, if $\langle g \rangle$ is synchronizing, then so is $\langle f, g \rangle$ for any $f \in T_n$; but $\langle f, g \rangle \neq T_n$, since T_n requires at least three generators.

3 Monoids and graphs

There is a very close connection between transformation monoids and graphs which we define in this section. It has some features of a Galois correspondence, but things are not quite so simple.

Let $\Omega = \{1, \dots, n\}$. We define maps in each direction between transformation monoids on Ω and graphs on the vertex set Ω .

One direction is well-known. Given a graph X , an *endomorphism* of X is an endofunction on Ω which maps edges of X to edges. (We do not care what it does to non-edges, which may be mapped to non-edges or to edges or to single vertices). The endomorphisms of X clearly form a monoid $\text{End}(X)$.

In the other direction, given a transformation monoid M , we define a graph $X = \text{Gr}(M)$ by the rule that two vertices v, w are adjacent if and only if there does not exist $f \in M$ such that $vf = wf$.

Not every graph occurs as the graph of a monoid. Recall that the *clique number* $\omega(X)$ is the cardinality of the largest complete subgraph of X , and the *chromatic number* $\chi(X)$ is the smallest number of colors required for a proper colouring of the vertices (so that adjacent vertices have different colours). Clearly $\omega(X) \leq \chi(X)$, since all vertices in a clique must have different colours; these parameters may differ arbitrarily.

Theorem 3.1 *For any transformation monoid M , $\omega(\text{Gr}(M)) = \chi(\text{Gr}(M))$, and this number is equal to the minimum rank of an element of M .*

Proof Let f be an element of M of minimum rank, and let S be the image of f . Then the induced subgraph on S is a clique; for if $v, w \in S$ are not adjacent, then there exists $g \in M$ with $vg = wg$, so that fg has smaller rank than f . But the map f is a proper colouring of $\text{Gr}(M)$, since by definition the images of adjacent vertices are distinct. So we have $\chi(\text{Gr}(M)) \leq |S| \leq \omega(\text{Gr}(M))$, whence equality holds throughout.

Corollary 3.2 (a) *$\text{Gr}(M)$ is a complete graph if and only if $M \leq S_n$ (that is, all elements of M are permutations).*

(b) *$\text{Gr}(M)$ is a null graph if and only if M is synchronizing.*

(c) *If $M_1 \leq M_2$, then $\text{Gr}(M_2)$ is a spanning subgraph of $\text{Gr}(M_1)$.*

The first and third parts, and the reverse implication in the second, are clear; the forward implication in the second part follows immediately from the preceding Theorem.

The two maps (from graphs to monoids and from monoids to graphs) are not mutually inverse, and do not (quite) form a Galois connection; but they do satisfy the following:

Theorem 3.3 *For any transformation monoid M ,*

- (a) $M \leq \text{End}(\text{Gr}(M))$;
- (b) $\text{Gr}(\text{End}(\text{Gr}(M))) = \text{Gr}(M)$.

Proof (a) Let $f \in M$, and let $\{v, w\}$ be an edge in $\text{Gr}(M)$. By definition, $vf \neq wf$. Could vf and wf be non-adjacent in $\text{Gr}(M)$? If so, then there would be $g \in M$ such that $(vf)g = (wf)g$. But then the map $fg \in M$ satisfies $v(fg) = w(fg)$, contradicting the fact that v and w are joined. So $f \in \text{End}(\text{Gr}(M))$.

(b) If $\{v, w\}$ is an edge of $\text{Gr}(M)$, then no endomorphism of $\text{Gr}(M)$ collapses it to a point, and so $\{v, w\}$ is an edge of $\text{Gr}(\text{End}(\text{Gr}(M)))$. Conversely, suppose that v and w are not adjacent in $\text{Gr}(M)$. Then by definition there exists $f \in M$ such that $vf = wf$. Since $f \in \text{End}(\text{Gr}(M))$ by (a), we see that v and w are not adjacent in $\text{Gr}(\text{End}(\text{Gr}(M)))$. So these two graphs are equal.

Given a graph X , the graph $\text{Gr}(\text{End}(X))$ is called the *hull* of X , and is studied in [2]. Theorem 3.3(b) shows that $\text{Hull}(\text{Hull}(X)) = \text{Hull}(X)$. In other words, a graph X is a hull if and only if it is its own hull (that is, $\text{Hull}(X) = X$).

4 Another construction

Here is another construction which doesn't decrease the endomorphism monoid of a graph.

Proposition 4.1 *Let X be a graph on the vertex set Ω with $\omega(X) = m$. Let X' be the spanning subgraph of X which consists of those edges of X which are contained in cliques of size m . Then $\text{End}(X) \leq \text{End}(X')$.*

Proof Suppose not. Then there exists $f \in \text{End}(X)$ such that $f \notin \text{End}(X')$. This means that there is an edge $\{v, w\}$ of X' such that either $vf = wf$, or $\{vf, wf\}$ is a non-edge of X' .

The first case is impossible since $\{v, w\}$ is an edge of X and $f \in \text{End}(X)$. Suppose that the second case happens. Then $\{vf, wf\}$ is an edge of X , and was deleted because it is not contained in any clique of size m . But $\{v, w\}$ is not deleted, so lies in a clique C of X with $|C| = m$; and then Cf is a clique of X with $\{vf, wf\} \subseteq Cf$ and $|Cf| = m$, a contradiction.

I will call Y the *derived graph* of X .

5 Maximal non-synchronizing monoids

In this section we will give a description of the maximal non-synchronizing monoids in terms of graphs. Note that, if the graph X is non-null, then $\text{End}(X)$ is non-synchronizing. The main theorem is the following:

Theorem 5.1 *Let M be a maximal non-synchronizing submonoid of T_n . Then there are graphs X and Y on the vertex set $\Omega = \{1, \dots, n\}$ satisfying the following conditions:*

- (a) $\text{End}(X) = \text{End}(Y) = M$;
- (b) $\omega(X) = \omega(Y) = \chi(X) = \chi(Y)$;
- (c) $X = \text{Hull}(Y)$;
- (d) $Y = X'$.

Proof Let M be maximal non-synchronizing. Let $X = \text{Gr}(M)$ and $Y = X'$. Then X has at least one edge (by Corollary 3.2(b)), and satisfies $\omega(X) = \chi(X)$ (by Theorem 3.1). Moreover, $M \leq \text{End}(X)$, by Theorem 3.3(a); maximality of M implies that equality holds.

Now $M = \text{End}(X) \leq \text{End}(Y)$ by Proposition 4.1; maximality of M implies that equality holds. Furthermore, it is clear that

$$\omega(Y) = \omega(X) = \chi(X) \geq \chi(Y) \geq \omega(Y),$$

so equality holds throughout. Finally, since $\text{End}(X) = \text{End}(Y)$, we see that

$$X = \text{Hull}(X) = \text{Gr}(\text{End}(X)) = \text{Gr}(\text{End}(Y)) = \text{Hull}(Y).$$

I do not know any examples where X and Y are not equal. If they are equal, then the converse holds:

Theorem 5.2 *Let X be a hull (other than the null graph), in which every edge is contained in a clique of size $\omega(X)$. Then $\text{End}(X)$ is a maximal non-synchronizing submonoid of $T(\Omega)$.*

Proof Let f be any endofunction not in $M = \text{End}(X)$. By Corollary 3.2(b), it suffices to show that for any $v, w \in \Omega$, there is an element $g \in M' = \langle M, f \rangle$ such that $vg = wg$. Since X is a hull, this holds for any v, w for which $\{v, w\}$ is a non-edge of X , so we may assume that $\{v, w\}$ is an edge.

I claim that, if $\{v', w'\}$ is another edge, then there is an endomorphism h of X satisfying $vh = v'$ and $wh = w'$. For, by assumption, there is a clique C with $|C| = \omega(X)$ containing v' and w' ; now there is an endomorphism from X onto C , and since C is complete, we may order its elements arbitrarily, so that in particular the images of v and w are v' and w' as claimed.

Since f is not an endomorphism, there is an edge $\{x, y\}$ of X such that either $xf \neq yf$, or $\{xf, yf\}$ is a non-edge. Composing f with an endomorphism if necessary, we may assume that $xf \neq yf$. Taking $v' = x$ and $w' = y$, and composing h of the preceding paragraph with f , we find an element of M with the required property.

There are many graphs satisfying the hypotheses of this theorem. The smallest consists of a single edge; there are $n(n-1)/2$ graphs of this form and each has $2n^{n-2}$ endomorphisms. So the probability that a random pair of endofunctions are both endomorphisms of a graph of this form is at most

$$\frac{n(n-1)}{2} \frac{n^{2(n-2)}}{n^{2n}} = O(n^{-2}).$$

This suggests that the probability that two random endofunctions generate a synchronizing monoid is at least $1 - O(1/n^2)$. However, we are still some way from a proof, since there are many graphs that need to be considered. Of course, there are big overlaps between their endomorphism monoids, so inclusion-exclusion will have to be applied much more carefully than in the case of Dixon's Theorem.

6 Open problems

The main problem is to prove that the probability that two random elements generate a synchronizing monoid is $1 - o(1)$.

A variant is to choose $r + s$ elements, of which r are random permutations and the remaining s are random endofunctions. If $r \geq 2$ and $s \geq 1$, then by Dixon's Theorem the permutations generate S_n or A_n with high probability, and the entire monoid is synchronizing with high probability. The interesting case here is $r = s = 1$.

A final problem is whether the two graphs in Theorem 5.1 can be distinct. If not, then the conditions of Theorem 5.2 would be necessary and sufficient for a monoid to be maximal non-synchronizing.

References

- [1] László Babai, The probability of generating the symmetric group, *J. Combinatorial Theory Ser. A* **52** (1989), 148–153.
- [2] Peter J. Cameron and Priscila A. Kazanidis, Cores of symmetric graphs, *J. Australian Math. Soc.* **85** (2008), 145–154.
- [3] John D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969) 199–205.
- [4] Tomasz Łuczak and László Pyber, On random generation of the symmetric group, *Combinatorics, Probability & Computing* **2** (1993), 505–512.